United States Government Accountability Office

GAO

Testimony

Before the Committee on Armed Services, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Wednesday, April 16, 2008

DEPARTMENT OF DEFENSE

Observations on the National Industrial Security Program

Statement of Ann Calvaresi Barr, Director
Acquisition and Sourcing Management

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
16 APR 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Department of Defense. Observations on the National Industrial Security Program	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**15**	

April 16, 2008

DEPARTMENT OF DEFENSE

Observations on the National Industrial Security Program

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-08-695T, a testimony before the House Armed Services Committee

Why GAO Did This Study

The National Industrial Security Program (NISP) aims to ensure contractors appropriately safeguard the government's classified information. NISP, along with other laws, regulations, policies, and processes, is intended to protect technologies critical to maintaining military technological superiority and other U.S. national security interests.

The Defense Security Service (DSS) within the Department of Defense (DOD) administers NISP on behalf of DOD and other federal agencies. DSS grants clearances to contractor facilities so they can access and, in some cases, store classified information. In 2005, DSS monitored over 11,000 facilities' security programs to ensure that they meet NISP requirements for protecting classified information.

In 2004 and 2005, GAO issued reports that examined DSS responsibilities related to facilities accessing or storing classified information. The first report assessed DSS oversight of facilities and DSS actions after possible compromises of classified information. The second focused specifically on DSS oversight of contractors under foreign ownership, control, or influence (FOCI). This testimony summarizes the findings of these reports and their relevance to the effective protection of technologies critical to U.S. national security interests—an area GAO designated as a governmentwide high-risk area in 2007.

To view the full product, including the scope and methodology, click on GAO-08-695T. For more information, contact Ann Calvaresi Barr at (202) 512-4841 or calvaresibarra@gao.gov.

What GAO Found

DSS did not systematically collect and analyze the information needed to assess its oversight of both contractor facilities and contractors under FOCI. While DSS maintained files on contractor facilities' security programs and their security violations, it did not use this information to determine, for example, whether certain types of violations are increasing or decreasing and why. As a result, DSS was unable to identify patterns of security violations across all facilities based on factors such as the type of work conducted, the facilities' government customer, or the facilities' corporate affiliation. Identifying such patterns would enable DSS to target needed actions to reduce the risk of classified information being compromised. With regard to contractors under FOCI, DSS did not collect and track the extent to which classified information was left in the hands of such contractors before measures were taken to reduce the risk of unauthorized foreign access. GAO found instances in which contractors did not report foreign business transactions to DSS for several months.

DSS's process for notifying government agencies of possible compromises to their classified information has also been insufficient. When a contractor facility reports a violation and the possible compromise of classified information, DSS is required to determine whether a compromise occurred and to notify the affected government agency so it can assess any damage and take actions to mitigate the effects of the suspected compromise or loss. However, for nearly 75 percent of the 93 violations GAO reviewed, DSS either made no determination regarding compromise or made a determination that was inconsistent with established criteria. In addition, in many cases in which DSS was required to notify the affected agencies of possible information compromises, the notification took more than 30 days; in one case, notification was delayed 5 months.

Despite the complexities involved in overseeing contactor facilities and contractors under FOCI, DSS field staff lacked the guidance, tools, and training necessary to effectively carry out their responsibilities. According to DSS field staff, they lacked research tools and training to fully understand, for example, the significance of corporate structures, legal ownership, and complex financial relationships when foreign entities are involved—knowledge that is needed to effectively oversee contractors under FOCI. Staff turnover and failure to implement guidance consistently also detracted from field staff's ability to effectively carry out responsibilities.

GAO has made numerous recommendations aimed at improving NISP and DSS's oversight of classified information that has been entrusted to contractors. Continued weaknesses in this and other areas that require rigorous oversight—such as export control, foreign acquisitions of U.S. companies, and foreign military sales—prompted GAO to designate the protection of critical technologies as high risk.

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss our work on the National Industrial Security Program (NISP), which aims to ensure contractors adequately safeguard the government's classified information. The Defense Security Service (DSS) within the Department of Defense (DOD) administers NISP on behalf of DOD and other federal agencies. DSS grants clearances to contractor facilities so they can access and, in some cases, store classified information. In 2005, DSS monitored over 11,000 facilities' security programs to ensure that they met NISP requirements for protecting classified information. We have issued two reports that examined how DSS carried out its industrial security responsibilities. The first report assessed DSS oversight of contractor facilities and DSS actions after possible compromises of classified information. The second focused specifically on DSS oversight of contractors under foreign ownership, control, or influence (FOCI).[1]

Before I discuss our work on NISP, I would like to place the program in a larger context. NISP is just one element within a myriad of laws, regulations, policies, and processes intended to identify and protect technologies critical to maintaining U.S. technological superiority on the battlefield and to provide for the transfer of these technologies to foreign parties in a manner consistent with U.S. economic, foreign policy and national security interests. The government's other technology protection programs include export control regimes, national security reviews of foreign acquisitions of U.S. companies, the foreign military sales program, the national disclosure policy process, and DOD's anti-tamper policy. Over the past several years GAO has looked at each of these and identified weaknesses in their implementation. These weaknesses have been exacerbated by the increasingly globalized nature of the defense industrial base and the increased pace of technological innovation worldwide. As a result, in 2007, we designated the effective protection of technologies critical to U.S. national security interests as a governmentwide high-risk area, which warrants a strategic reexamination of existing programs to identify needed changes and better ensure the advancement of U.S. interests. I believe this hearing today contributes to that strategic reexamination.

[1]GAO, *Industrial Security: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information*, GAO-04-332 (Washington, D.C.: Mar. 3, 2004), and *Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient*, GAO-05-681 (Washington, D.C.: July 15, 2005).

This testimony is based on the cited reports, which were done in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Summary

Our work on DSS oversight of contractor facilities and DSS oversight of contractors under FOCI identified certain systemic weaknesses. In both areas DSS did not systematically collect and analyze information to assess the effectiveness of its operations. Such an assessment would have assisted DSS in better managing its processes and enabled it to identify problems and institute corrective actions. In terms of facility oversight, DSS maintained files on contractor facilities' security programs and their security violations, but it did not analyze this information to determine, for example, whether certain types of violations are increasing or decreasing and why. Further, the manner in which this information was maintained—geographically dispersed paper-based files—did not lend itself to this type of analysis. As a result, DSS was unable to identify patterns of security violations across all facilities based on factors such as the type of work conducted, the facilities' government customer, or the facilities' corporate affiliation. Identifying such patterns would enable DSS to target needed actions to reduce the risk of classified information being compromised. Similarly, DSS did not systematically collect or analyze information on foreign business transactions in a manner that helped it properly oversee contractors entrusted with U.S. classified information. Specifically, DSS did not know the universe of contractors operating under protective measures. With regard to contractors under FOCI, DSS did not collect and track in a timely manner the extent to which classified information was left in the hands of such contractors before measures were taken to reduce the risk of unauthorized foreign access. Specifically, we found instances in which contractors did not report foreign business transactions to DSS until several months after they had occurred.

DSS's process for notifying government agencies of possible compromises of their classified information has also been insufficient. When a contractor facility reports a violation and the possible compromise of classified information, DSS is required to determine whether compromise occurred and to notify the affected government agency so it can assess any damage and take actions to mitigate the effects of the suspected compromise or loss. However, for nearly 75 percent of the 93 violations

GAO reviewed, DSS either made no determination regarding compromise or made inappropriate determinations, such as "compromise cannot be precluded" or "compromise cannot be determined"—neither of which are covered by established criteria. In addition, in many cases in which DSS was required to notify the affected agencies of possible information compromises, the notification took more than 30 days; in one case, notification was delayed 5 months.

Finally, we found that DSS field staff lacked the guidance, tools, and training necessary to effectively carry out their responsibilities. DSS field staff faced a number of challenges that significantly limited their ability to sufficiently oversee contractors under FOCI. Field staff told us they lacked research tools and training to fully understand the significance of corporate structures, legal ownership, and complex financial relationships when foreign entities are involved. Staff turnover and inconsistencies over how guidance was to be implemented also detracted from field staff's ability to effectively carry out FOCI responsibilities.

Although in its initial response to our reports, DOD did not agree with many of our recommendations or the need for corrective actions, we understand that DSS has subsequently begun to address some of the issues we raised.

Background

NISP was established by executive order in 1993[2] to replace industrial security programs operated by various federal agencies. The goal of the national program is to ensure that contractors' security programs detect and deter espionage and counter the threat posed by adversaries seeking classified information. Contractor facilities must be cleared prior to accessing or storing classified information and must implement certain safeguards to maintain their clearance. The National Industrial Security Program Operating Manual (NISPOM) prescribes the requirements, restrictions, and safeguards that contractors are to follow to prevent the unauthorized disclosure—or compromise—of classified information.

DSS is responsible for providing oversight, advice, and assistance to U.S. contractor facilities that are cleared for access to classified information. Contractor facilities can range in size, be located anywhere in the United

[2]Executive Order no. 12829, signed January 6, 1993, established NISP for the protection of information classified under Executive Order 12958, as amended.

States, and include manufacturing plants, laboratories, and universities. Industrial security representatives work out of DSS field offices across the United States and serve as the primary points of contact for these facilities. Representatives' oversight involves educating facility personnel on security requirements, accrediting information systems that process classified information, approving classified storage containers, and assisting contractors with security violation investigations. DSS representatives also conduct periodic security reviews to assess whether contractor facilities are adhering to NISPOM requirements and to identify actual and potential security vulnerabilities.

Contractors are required to self-report foreign business transactions on a Certificate Pertaining to Foreign Interests form.[3] Examples of such transactions include foreign ownership of a contractor's stock, a contractor's agreements or contracts with foreign persons, and whether non-U.S. citizens sit on a contractor's board of directors. Contractors are required to report changes in foreign business transactions and to update this certificate every 5 years. Because a U.S. company can own a number of contractor facilities, the corporate headquarters or another legal entity within that company is required to complete the certificate.[4]

When contractors declare foreign transactions on their certificates and notify DSS, industrial security representatives are responsible for ensuring that contractors properly identify all relevant foreign business transactions. They are also required to collect, analyze, and verify pertinent information about these transactions. For example, by examining various corporate documents, the industrial security representatives are to determine corporate structures and ownership and identify key management officials. The representatives may consult with DSS counterintelligence officials, who can provide information about threats to U.S. classified information. If contractors' answers on the certificates indicate that foreign transactions meet certain DSS criteria or exceed thresholds, such as the percentage of company stock owned by

[3]In this testimony we refer to information reported by contractors on the Certificate Pertaining to Foreign Interests as foreign business transactions.

[4]Each business structure has its own set of legal requirements. Within the NISP, the most common type of business structure is the corporation. A corporation may be organized as a single corporate entity, a multiple facility organization with divisions, or a parent-subsidiary relationship. Under a multiple facility organization, the home office is the legal entity, while the divisions are extensions of the legal entity. In a parent-subsidiary relationship, the parent and the subsidiary are separate legal entities.

foreign persons, the representatives forward these cases to DSS headquarters. DSS headquarters works with contractors to determine what, if any, protective measures are needed to reduce the risk of foreign interests gaining unauthorized access to U.S. classified information. Field staff are then responsible for monitoring contractor compliance with these measures.

DSS Did Not Systematically Collect and Analyze Information to Identify Weaknesses and Institute Corrective Actions

In overseeing contractor facilities and contractors under FOCI, DSS did not systematically collect and analyze information to assess the effectiveness of its operations. Without this analysis, DSS was limited in its ability to detect trends in the protection of classified information across facilities, to determine sources of security vulnerabilities, and to identify those facilities with the greatest risk of compromise. In addition, DSS was unable to determine whether contractors were reporting foreign business transactions as they occurred or how much time a contractor facility with unmitigated FOCI[5] had access to classified information.

In overseeing contractor facilities, we found DSS evaluated its performance in terms of process factors, such as the

- percentage of security reviews completed,
- percentage of security reviews that covered all pertinent areas of contractors' security programs,
- length of time needed to clear contractor facilities for access to classified information, and
- length of time needed to clear contractor personnel for access to classified information.

While such indicators are important, they alone cannot measure where the greatest risks are, the types of violations that are occurring, and by whom. Performance indicators such as the ratings[6] and number of findings[7] that resulted from security reviews would have provided an indication as to

[5]Unmitigated FOCI refers to situations in which contractors with facility clearances are under FOCI and protective measures are needed but not yet implemented.

[6]After a security review, an industrial security representative was to rate that facility's security program in terms of how well it met NISPOM requirements and ensured the protection of classified information.

[7]DSS defined a finding as the failure to comply with the NISPOM. Findings were either administrative or serious. Serious findings could lead to the loss or compromise of classified information.

whether DSS was achieving its mission. However, there were no such indicators to determine overall facility ratings, the sources of the violations, and their frequency. Without such information, DSS cannot ensure facilities are protecting the classified information entrusted to them.

Similarly, DSS did not know how many contractors under FOCI were operating under all types of protective measures and, therefore, was unaware of the magnitude of potential FOCI-related security risks. Although DSS tracked information on contractors operating under some types of protective measures, it did not centrally compile data on contractors operating under all types of protective measures. Specifically, DSS headquarters maintained a central repository of data on contractors under voting trust agreements, proxy agreements, and special security agreements—protective measures intended to mitigate majority foreign ownership. However, information on contractors under three other protective measures—security control agreements, limited facility clearances, and board resolutions—were maintained in paper files in the field offices. DSS did not aggregate data on contractors for all six types of protective measures and did not track and analyze overall numbers. Such analysis would allow DSS to target areas for improved oversight.

The NISPOM requires contractors with security clearances to report any material changes of business transactions previously notified to DSS. DSS is dependent on contractors to self-report transactions by filling out the Certificate Pertaining to Foreign Interests form. However, this form did not ask contractors to provide specific dates for when foreign transactions took place. Consequently, DSS did not know if contractors were reporting foreign business transactions as they occurred and lacked knowledge about how much time a contractor facility with unmitigated FOCI had access to classified information. In addition, DSS did not compile or analyze how much time passed before it became aware of foreign business transactions. DSS field staff told us that some contractors reported foreign business transactions as they occurred, while others reported transactions months later, if at all. During our review, we found a few instances in which contractors were not reporting foreign business transactions when they occurred. One contractor did not report FOCI until 21 months after awarding a subcontract to a foreign entity. Another contractor hired a foreign national as its corporate president but did not report to DSS, and DSS did not know about the change until 9 months later, when the industrial security representative came across the information on the contractor's Web site. In another example, DSS was not aware that a

foreign national sat on a contractor's board of directors for 15 months until we discovered it while conducting our audit work.

DSS also did not determine the time elapsed between the reporting of foreign business transactions by contractors with facility clearances until the implementation of protective measures or when suspensions of facility clearances occurred. Without protective measures in place, unmitigated FOCI at a cleared contractor increases the risk that foreign interests can gain unauthorized access to U.S. classified information. We found two cases in which contractors appeared to have operated with unmitigated FOCI before protective measures were implemented. For example, officials at one contractor stated they reported to DSS that their company had been acquired by a foreign entity. However, the contractor continued operating with unmitigated FOCI for at least 6 months. According to the NISPOM, DSS shall suspend the facility clearance of a contractor with unmitigated FOCI, and DSS relies on field office staff to make this determination. Contractor officials in both cases told us that their facility clearances were not suspended. Because information on suspended contractors with unmitigated FOCI is maintained in the field, DSS headquarters did not determine at an aggregate level the extent to which and under what conditions it suspends contractors' facility clearances due to unmitigated FOCI.

Many Determinations of Information Compromise either Did Not Occur or Were Done Inappropriately

Industrial security representatives often failed to determine whether security violations by facilities resulted in the loss, compromise, or suspected compromise of classified information or made determinations that were not in accordance with approved criteria. Determinations of loss, compromise, or suspected compromise are important because the affected government customer must be notified so it can evaluate the extent of damage to national security and take steps to mitigate that damage. Even when representatives made an appropriate determination, they often took several weeks and even months to notify the government customer because of difficulties in identifying the customer. As a result, the customer's opportunity to evaluate the extent of damage and take necessary corrective action was delayed.

The NISPOM requires a facility to investigate all security violations. If classified information is suspected of being compromised or lost, the facility must provide its DSS industrial security representative with information on the circumstances of the incident and the corrective actions that have been taken to prevent future occurrences. The industrial security representative is to then review this information and, using the

criteria specified in DSS's Industrial Security Operating Manual, make one of four final determinations: no compromise, suspected compromise, compromise, or loss.

If a determination other than no compromise is made, the Industrial Security Operating Manual directs the representative to inform the government customer about the violation so a damage assessment can be conducted. However, for 39 of the 93 security violations that we reviewed, industrial security representatives made no determination regarding the compromise or loss of classified information. For example, in two cases involving one facility, the representative made no determination of compromise even though the facility reported the improper transmission of classified information via e-mail. In another eight cases at another facility, the representative made no determination despite employees' repeated failure to secure a safe room to ensure the protection of classified information. In the absence of a determination, the government customers were not notified of these violations and therefore were unable to take steps to assess and mitigate any damage that may have occurred.

For the remaining 54 violations that we reviewed, representatives made determinations regarding the compromise or loss of information, but many were not consistent with the criteria contained in DSS's Industrial Security Operating Manual. Representatives made 30 inappropriate determinations, such as "compromise cannot be precluded" or "compromise cannot be determined." For example, in nine cases, the same facility reported that classified material was left unsecured, and the facility did not rule out compromise. In each of these cases, the industrial security representative did not rule out compromise but used an alternative determination. Senior DSS officials informed us that industrial security representatives should not make determinations other than the four established in the Industrial Security Operating Manual because the four have specific meanings based on accepted criteria. By not following the manual, representatives introduced variability in their determinations and, therefore, their decisions of whether to notify the government customer of a violation.

The failure of representatives to always make determinations consistent with the Industrial Security Operating Manual was at least partially attributable to inadequate oversight. The Standards and Quality Branch is the unit within DSS responsible for ensuring that industrial security representatives properly administer the NISP. Branch officials regularly test and review field office chiefs and representatives on NISP requirements, particularly those related to granting clearances and conducting security reviews. However, the Standards and Quality Branch

did not test or review how representatives responded to reported violations and made determinations regarding compromise. As a result, DSS did not know the extent to which representatives understood and were consistently applying Industrial Security Operating Manual requirements related to violations and, therefore, could not take appropriate action.

While the Industrial Security Operating Manual did not specify a time requirement for notifying government customers when classified information had been lost or compromised, DSS was often unable to notify customers quickly because of difficulties in identifying the affected customers. DSS notified government customers regarding 16 of the 54 reported violations for which representatives made determinations. For 11 of these 16 violations, DSS did not notify the customer for more than 30 days after the contractor reported that information was lost, compromised, or suspected of being compromised. In one case, 5 months passed before an industrial security representative was able to notify a government customer that its information was suspected of being compromised. This delay was a result of the facility's inability to readily determine which government customer was affected by the compromise. DSS relied on the facility to provide this information. However, facilities that were operating as subcontractors often did not have that information readily available.

DSS Did Not Always Provide Adequate Guidance, Training, and Tools to Field Staff

DSS industrial security representatives faced several challenges in carrying out their FOCI responsibilities, largely due to complexities in verifying FOCI cases, limited tools to research FOCI transactions, insufficient FOCI training, staff turnover, and inconsistencies in implementing guidance on FOCI cases.

For industrial security representatives, verifying if a contractor is under FOCI is complex. Representatives are required to understand the corporate structure of the legal entity completing the Certificate Pertaining to Foreign Interests form and to evaluate the types of foreign control or influence that exist for each entity within a corporate family. For example, representatives are required to verify information on stock ownership by determining the distribution of the stock among the stockholders and the influence or control the stockholders may have within the corporation. This entails identifying the type of stock and the number of shares owned by the foreign person(s) to determine authority and management prerogatives. Some industrial security representatives told us they did not always have the tools needed to verify if contractors

are under FOCI. They conducted independent research using the Internet or returned to the contractor for more information to evaluate the FOCI relationships and hold discussions with management officials, such as the chief financial officer, treasurer, and legal counsel. DSS headquarters officials told us additional information sources, such as the Dun and Bradstreet database of millions of private and public companies were not available in the field.

In addition, industrial security representatives stated they lacked the training and knowledge needed to better verify and oversee contractors under FOCI. For example, DSS did not require its representatives to have financial or legal training. While some FOCI training was provided, representatives largely depended on DSS guidance and on-the-job training to oversee a FOCI contractor. In so doing, representatives worked with more experienced staff or sought guidance, when needed, from DSS headquarters.

Despite DSS efforts to provide training on FOCI, we found that the training needs on complex FOCI issues were still a concern to representatives. In fact, many said they needed more training to help with their responsibility of verifying FOCI information, including how to review corporate documents, strategic company relationships, and financial reports. In addition, officials from one-third of the field offices we reviewed noted staff retention problems. DSS officials at two of these field offices said that in particular they have problems retaining more experienced industrial security representatives.

Compounding these challenges are inconsistencies among field offices in how industrial security representatives said they understood and implemented DSS guidance for reviewing contractors under FOCI. For example, per DSS guidance, security reviews and FOCI meetings should be performed every 12 months for contractors operating under special security agreements, security control agreements, voting trust agreements, and proxy agreements. However, we found that some industrial security representatives did not follow the guidance. One representative said a contractor under a special security agreement was subject to a security review every 18 months because the contractor did not store classified information on-site. In addition, two industrial security representatives told us they did not conduct annual FOCI meetings for contractors that were operating under a proxy agreement and security control agreement, respectively. We also found that industrial security representatives varied in their understanding or application of DSS guidance for when they should suspend a contractor's facility clearance when FOCI was

unmitigated. The guidance indicates that when a contractor with a facility clearance is determined to be under FOCI that requires mitigation by DSS headquarters, the facility security clearance shall be suspended until a protective measure is implemented. However, we were told by officials in some field offices that they rarely suspend clearances when a contractor has unmitigated FOCI as long as the contractor is demonstrating good faith in an effort to provide documentation to DSS to identify the extent of FOCI and submit a FOCI mitigation plan to DSS. Officials in other field offices said they would suspend a contractor's facility clearance once they learned the contractor had unmitigated FOCI.

In conclusion, we believe that the weaknesses identified in the NISP and other programs designed to protect technologies critical to U.S. national security present significant challenges and need to be addressed. Although in its initial response to our reports, DOD did not agree with many of our recommendations or the need for corrective actions, we understand that DSS has subsequently begun to address some of the issues we raised. While we have not reviewed any of these actions and therefore can not address their potential effectiveness, we welcome DSS's recognition that action is needed.

Mr. Chairman this concludes my statement. I would be happy to answer any questions you or other members of the committee may have.

For information about this testimony, please contact Ann Calvaresi Barr, Director, Acquisition and Sourcing Management, at (202) 512-4841 or calvaresibarra@gao.gov. Other individuals making key contributions to this product include Thomas J. Denomme, Brandon Booth, John Krump, Karen Sloan, Lillian Slodkowski, and Suzanne Sterling.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "E-mail Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548